Electronic Version
Stylesheet Version v1.1.1

[Electronic Files Digital Rights Management.]

Abstract

This invention uses file hash signatures, including but not limited to those generated from MD5, MD2, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 and FIPS 180-2 files, and various file comparison and matching technologies in a real time or near real time solution to determine if digital content has been stolen or otherwise illegally, opened, transferred, viewed, played or copied. Once digital content has been analyzed (match or no match) one or more follow-on actions can be taken with respect to the content based on preferences established by the owner/authorized agent of the digital content. These include blocking the copy or playback process, preventing transferring of files over a network or between systems, notification to one or more users about the theft of illegal use and/or instruction(s) to the unauthorized user. Digital content includes but is not limited to digital audio, digital picture and video, and digital documentation. One method for using this invention is to match file hash signature(s) of file(s) that are being transferred, opened, or sampled by using an analytic con-

trol engine (ACE) to determine if any of those files match those known or suspected of being stolen. This can be done with or without a proprietary hash algorithm to accelerate the process of identifying matching hash signatures. Another use of this invention includes, but is not limited to, the integration of this invention into microchip technology including ASICs with external flash memory or with other microprocessors with built in or external flash memory that can store hash signatures in a database, flat file, or table which can be read and dynamically updated. This invention can also integrate into portable digital audio (Mp3, Mp4, AAC, AIFF, WMV, RP, and others) players and recorders to prevent digital content once identified as illegal or invalid from being played or transferred. Another use of this invention is with external storage adapters such as IEEE 1394A and IEEE 1394B Firewire and USB1.0 and USB2.0 connections to prevent the transfer of illegal digital content. This invention also applies to current and future adaptations of storage devices such as hard drives, CD and DVD readers, writers, and recorders, and other adapter interfaces including ATA, IDE, SCSI, Flash, and RAM devices.